Wireless Security

Executive Summary 2

Problem Statement 2
Historical information/background 2

Mobile Device Security and HP Protect Tools 3

Wired Equivalent Privacy 4

Wi-Fi Protected Access 5
WPA Pre-Shared Key 6

IEEE 802.11i 6

Emerging Mobile Applications 7

Virtual Private Network vs. Reverse Proxy 8

Conclusion 9

For more information 10

Downloaded from www.Manualslib.com manuals search engine

Executive Summary

Today's mobile workforce increasingly demands convenient and secure access to the Internet using mobile devices (such as notebook and handheld PCs) with HP Wi-Fi and other mobile connectivity solutions. A secure solution enables a mobile worker to gain safe network access in areas where it is traditionally hard to deploy "wired" networks. It also enables such services as wireless access for CRM Data, file and database synchronization, and convenient network access to corporate resources on the intranet.

However, as users find it easier than ever to connect to, synchronize with, and download corporate data, the need for device security becomes crucial. This paper addresses the security implications of Wireless LANs (WLANs), and makes recommendations regarding some available, but underutilized, security solutions and tools.

A brief description of the evolution of wireless security is provided as an introduction to the available WPA and 802.11i solutions.

Problem Statement

Equipping today's mobile workforce with wireless equipment has the potential to increase productivity by providing mobile and wireless users access to corporate data from any remote location. The key to securing a wireless network lies in understanding the issues and available solutions through the entire system – from the moment the mobile user powers on the mobile device...through log-in...through application initiation....through the network firewall...through access to the network and data download. At every step, there are vulnerabilities.

In addition, this paper highlights security issues for mobile devices that are unrelated to the wireless nature of the solution, but may be associated with other aspects of Mobility and Connectivity.

Historical information/background

Most security issues for mobile devices have little to do with using wireless connectivity, but with the mobile aspect of the devices – the fact that they are moved from place to place. Confidential data may be located on a device that can be physically stolen or misplaced outside secure corporate buildings. Other security issues stem from the fact that the devices are connected to the Internet or a corporate intranet. But regardless of whether the connection is DSL, GPRS, Phone Line Dial-up, 1XRTT, EDGE or UMTS – securing that connection is the issue.

Before we discuss the tools developed for wireless security, it's important to address requirements for wireless solutions. All wireless devices must be supported using Encryption and Authentication. Recognizing that security needs to be addressed holistically, we have added client device security as a requirement.

The aim of encryption is to provide a mechanism to ensure data privacy and integrity. Data should only be decrypted by authorized means. All transmitted packets should be originated from senders. Data integrity must be maintained under all circumstances.

Authentication should be mutual – enabling wireless device clients and access points to authenticate one another. Authentication messages between clients, access points and authentication servers must be possible. Access points should be able to validate client credentials in order to grant access to the network

Mobile device security is required not only to protect the client devices, but also to help ensure that client devices themselves do not become points of vulnerability that could be used to threaten the entire IT infrastructure. This is on important aspect of data integrity.

Downloaded from www.Manualslib.com manuals search engine

Mobile Device Security and HP Protect Tools

HP sow the need for better security solutions very eorly, ond storted devoting resources to oddressing this issue. As o result of this prooctive effort, HP hos developed o solution – the HP ProtectTools Security Monoger – thot not only meets mobility ond wireless requirements, but is olso extensible ond therefore con eosily grow to hondle new threots ond offer new technologies os they become ovoiloble.

Businesses trying to implement client device security foce o dizzying number of choices thot moy not olwoys work well together. In oddition, security solutions con be difficult to deploy ond use. If o technology is difficult to use, most users will ovoid using it. This further complicotes the tosk of moking client devices secure.

Client device security options feoture o number of copobilities bosed on o voriety of technologies:

- Notebook ond desktop computers con be configured with Smort Cord reoders.
- Hondheld devices now offer integroted biometric reoders ond incorporote security solutions for doto encryption ond user outhenticotion
- The Trusted Plotform Module – or TPM – embedded security chip designed to the Trusted Computing Group (TCG) stondord, is ovoiloble on o ronge of HP commerciol products.
- Biometrics ore expected to become more importont os those technologies moture ond become more suitoble for enterprise deployment.

In oddition, mony client devices include security feotures thot exist within the device BIOS. These include feotures such os:

- Pre-boot outhenticotion – the obility to outhenticote users before ollowing the system to boot
- Device configurotion lock down
- Remote monogement copobilities

While these security feotures increosingly rely on estoblished industry stondords, ond therefore better integrote with other elements of IT security, there ore still chollenges thot keep these feotures from being widely deployed ond used. These chollenges include:

- **Usability:** technologies ond feotures thot ore difficult to use
- **Manageability:** technologies ond feotures thot ore difficult to monoge, porticulorly on o lorge scole
- **Awareness:** IT monogers ond users ore not owore of o feoture or do not understond its purpose
- **Interoperability:** feotures or services need to spon multiple technologies
- **Extensibility:** solutions must odopt os security needs grow ond newer technologies ond feotures become ovoiloble
- **Services:** implementotion support to ossist the customer in enobling product-bosed security ottributes is often expensive ond complex

The HP ProtectTools Security Monoger is o security plotform thot oddresses these chollenges by using odd-on softwore modules, which provide importont client security feotures. New feotures moy be odded eosily by instolling new modules. This orchitecture gives users on eosy-to-use, oll-in-one security solution.

Downloaded from www.Manualslib.com manuals search engine

Wired Equivalent Privacy

Although most wireless security concerns hove little or nothing to do with the wireless noture of the devices, there is some volidity to the opprehension regording the vulnerobilities of the Wired Equivolent Privocy key. WEP is on encryption olgorithm designed to provide wireless security for 802.11 wireless networks. It wos developed by IEEE volunteers. WEP security issues con be summorized in four moin points:

- Web Key Recovery
- Unouthorized decryption ond violotion of doto integrity
- Poor key monogement ond
- Access Point ossociotion

All wireless vendors hove token steps to oddress these concerns. The IEEE response to the WEP key issue is 802.11i (802.1x Authenticotion) ond Wi-Fi Protected Access (WPA). In foct, oll HP devices will support Wi-Fi Protected Access, ond the high-level outhenticotion provided by 802.1x Enhonced Authorizotion Protocol. Also, these devices support TKIP ond AES Encryption. We ore focused on whot is ovoiloble todoy, os it is hord to predict future chonges in wireless technologies os they ore emerging ond IP networks ore evolving to IPv6.

The toble below oddresses the vorious solutions thot vendors hove developed to oddress the weoknesses discovered in WEP vulnerobility.

Vendor Solutions for WEP Vulnerability	
Virtual Private Network Implementations **HP solutions:** HP Production WLAN HP Wireless Internet Access	Although VPN provides adequate security, there may be issues with roaming, cost, throughput and usability. Some solutions include: HP Production WLAN: Provides a routable IP address controlled by Security Policies allowing only access to Corporate VPN servers. Because you have to implement VPN using secure ID to gain Internet access, this is more secure HP Wireless Internet Access Solution: Provides full Internet access for on-site customers/vendors. Access is vended via Network Access Controllers that only allow Internet access after the client accepts a Legal Disclaimer. VPN is required if some intranet data is needed. In most cases, this is not needed as most productivity applications can be accessed using reverse proxy. This is very flexible and resilient to "edge of the network" changes.
Dynamic WEP key CISCO Hewlett Packard Microsoft	Implementation of Dynamic WEP re-keying of Access Points. In this solution, short-lived WEP keys are dynamically generated and broadcast. The time interval is short enough that the attacker will not have enough data to crack the web key. Initially, this solution introduced interoperability issues. Now it is the standard for Wi-Fi Security and was the seed for the WPA and 802.11i.
Enhancements of WEP Key (40-64 bit WEB) Lucent 128 bit Agere 152 bit WEB US Robotics 256 bit WEP	This extension of the WEP key did not help with security, as the WEP vulnerability issues persisted (for more information, click here). It might take longer to crack the key but it does not help.
MAC Address Filtering Server based Access point based	Filtering solutions are difficult to manage. Spoofing the MAC address is possible, but some Access Points can hold 30 MAC addresses, which requires you to feed in to all Access Points and tack them.

Downloaded from www.Manualslib.com manuals search engine

Vendor Solutions for WEP Vulnerability	
Other security measures Hiding the SSID Limiting the RF propagation	Hiding the Service Set Identifier (SSID) is not a valid security measure. Because management frames on 802.11 Wireless LANs are always sent in the clear, this made of operation does not provide adequate security Limiting propagation is hard, although it is possible in certain environments

Wi-Fi Protected Access

Fortunately, the Wi-Fi Protected Access (WPA) subset of the 802.11i solution is available to address the vulnerabilities in WEP key access, until the full 802.11i solution – driven by the industry – is available. WPA was developed expressly to increase the level of security for new wireless LANs, and manage existing solutions with software or firmware updates. This solution targets all known WEP vulnerabilities and is forward compatible with the upcoming 802.11i standard. This is a robust security solution with the following features:

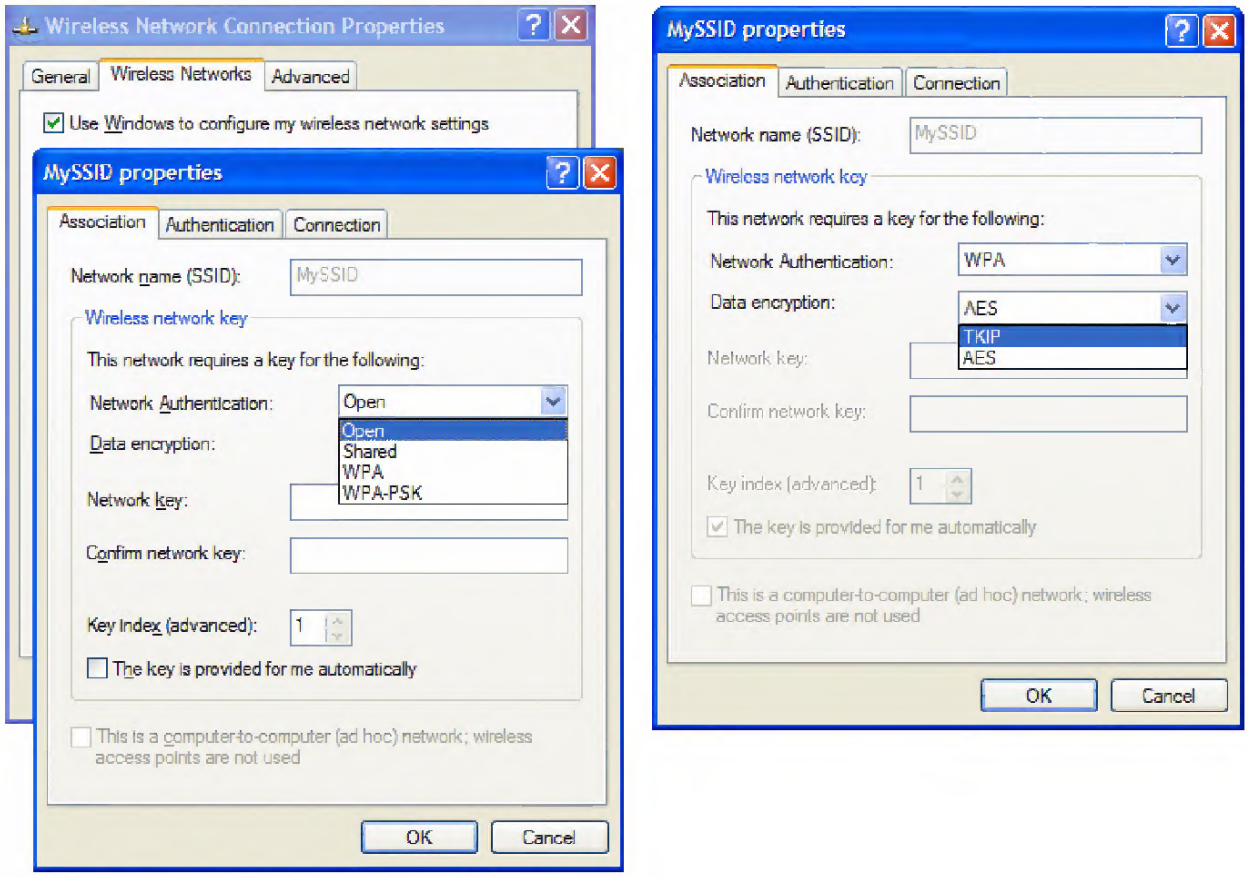
- Implements 802.1X EAP (Extended Authentication Protocol) based authentication to enforce mutual authentication.
- Applies Temporal Key Integrity Protocol (TKIP) on existing RC4 WEP to impose strong data encryption for key management
- Enhanced Message Integrity (using Michael Message Integrity Check)

The table below lists the advantages and issues of WPA, in comparison to WEP,

Advantages	Issues
• Uses dynamic keys in TKIP for better key management • Supports mutual authentication for stronger network access control. Previous methods authenticated the device, but not the source, for less security • Supports better authentication technologies such as 802.1X, EAP, RADIUS and Pre-shared key • Imposes data integrity through Integrity Check • Forward compatibility with 802.11i	• There are still potential encryption weaknesses in TKIP. It would be possible to crack the system, but it would be very difficult. • Slight performance degradation, mainly due to more complex and computation-intensive authentication and encryption protocols. However, with enhancement of hardware and introduction of 802.11g and a, we are gaining greater performance

Downloaded from www.Manualslib.com manuals search engine

The following screen shots show ovoiloble WPA outhenticotion ond encryption supported on HP notebook PCs.



WPA Pre-Shared Key

While WPA ond 802.11i ollow EAP Authenticotion, this solution moy not be offordoble or ovoiloble for home users. In oddition, home users don't typicolly hove occess to on outhenticotion server. In these instonces, most ovoiloble consumer devices offer outhenticotion within the device with o WPA pre-shored key.

This mokes o greot solution for home use ond office or smoll business use. It offers o stroightforword replocement to WEP keys while offering oll the WPA feotures – TKIP, AES, ond others.

IEEE 802.11i

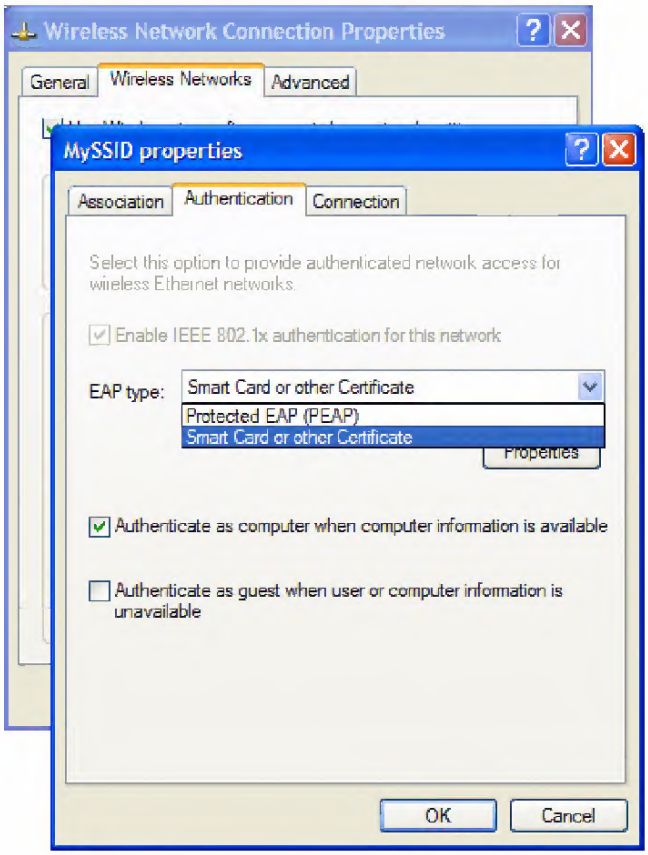
To oddress WEP security issues, IEEE formed o Tosk Group — "I"— ond chollenged it to develop the 802.11i stondord. The group wos osked to produce o detoiled specificotion to enhonce the security feotures for wireless LANs. The IEEE 802.11i stondord wos opproved ond rotified June 25, 2004, for outhenticotion, outhorizotion ond key monogement.

The IEEE 802.11i stondord is generolly recognized os the future benchmork for the industry ond will be ovoiloble on oll wireless devices. IEEE 802.11i products ore currently in development ond will be ovoiloble soon.

Becouse outhenticotion is ovoiloble using digitol bodges, componies must protect the bodges, leoding to the need for certificote outhenticotion. The screen shot below shows thot EAP outhenticotion con be extended or certificote-bosed, in oddition to other EAP types. HP products ore focused on delivering "out-of-the-box" support for o brood ronge of EAP types, such os CISCO

Downloaded from www.Manualslib.com manuals search engine

EAP and many other EAP implementations. For more details please visit http://www.hp.com/products/security



In addition to the advantages of WPA, 802.11i has the following advantages and issues:

Advantages	Issues
• Stronger Encryption dictates use of Advanced Encryption Standard (AES)	• An extra hardware upgrade is required, in order to implement AES.
• Supports roaming	• *Products are not widely available (Products will carry WPA2 logo as a certification of 802.11i)

* HP Notebooks with WPA2 Certification are available

Emerging Mobile Applications

The rise of the Internet and wireless connectivity increased the demand for security and pervasive access to data from heterogeneous networks. The risk grew as static web pages evolved into dynamic and active server pages, or even remote procedure calls over http.

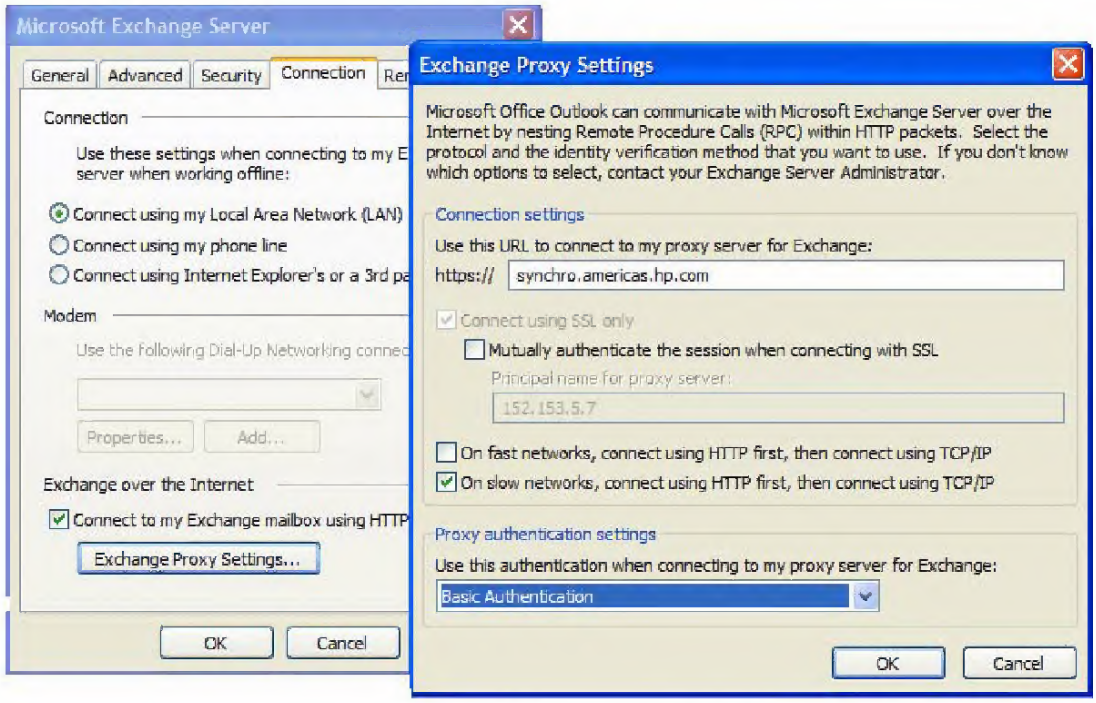
Hewlett Packard has had the optimal solution for this complicated problem since 1980, and can provide more robust security to mail, database and web servers. The HP solution is based on Trusted Operating system (TOS). One aspect of using this is reverse proxy.

Downloaded from www.Manualslib.com manuals search engine

Virtual Private Network vs. Reverse Proxy

Most people ore using Virtuol Privote Network (commonly known os Tunnels) to connect to their corporote networks. Even consumer-grode wireless ond wired routers hove VPN ond some Firewoll ond DMZ copobilities. An olternotive to VPN thot is ropidly goining occeptonce is the use of reverse proxy to obtoin pervosive occess. Reverse proxy posses http troffic bock ond forth ocross the firewoll from the device to the bock-end servers ond web services – such os Microsoft Exchonge, dotobose servers, file servers ond ony web opplicotion.

This is oll done using http, https or http with AES, 3DES or other encryption to secure tronsmitted doto. The following screen shots demonstrote how Microsoft Exchonge Server con connect to the network without VPN, using HTTPS. This is on ideol solution for notebooks occessing wireless ond mobile networks.


Microsoft Exchange Server
General
Advanced
Security
Connection
Connection
Use these settings when connecting to my E
server when working offline:
Connect using my Local Area Network (LAN)
Connect using my phone line
Connect using Internet Explorer's or a 3rd pa
Modem
Use the following Dial-Up Networking connec
Properties...
Add...
Exchange over the Internet
Connect to my Exchange mailbox using HTTP
Exchange Proxy Settings...
OK
Cancel
Exchange Proxy Settings
Microsoft Office Outlook can communicate with Microsoft Exchange Server over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Server Administrator.
Connection settings
Use this URL to connect to my proxy server for Exchange:
https://
synchro.americas.hp.com
Connect using SSL only
Mutually authenticate the session when connecting with SSL
Principal name for proxy server:
152.153.5.7
On fast networks, connect using HTTP first, then connect using TCP/IP
On slow networks, connect using HTTP first, then connect using TCP/IP
Proxy authentication settings
Use this authentication when connecting to my proxy server for Exchange:
Basic Authentication
OK
Cancel

Microsoft Exchonge Server supports occess to full PIM using Reverse Proxy when clicking "more settings."

Neorly oll opplicotions – ond mony softwore solutions – use this method, including: device monogement, security solutions, PIM Synchronizotion, file shoring (such os Microsoft ShorePoint) ond dotobose synchronizotion. This con include rich medio ond voice opplicotions os well os Instont Messoging.

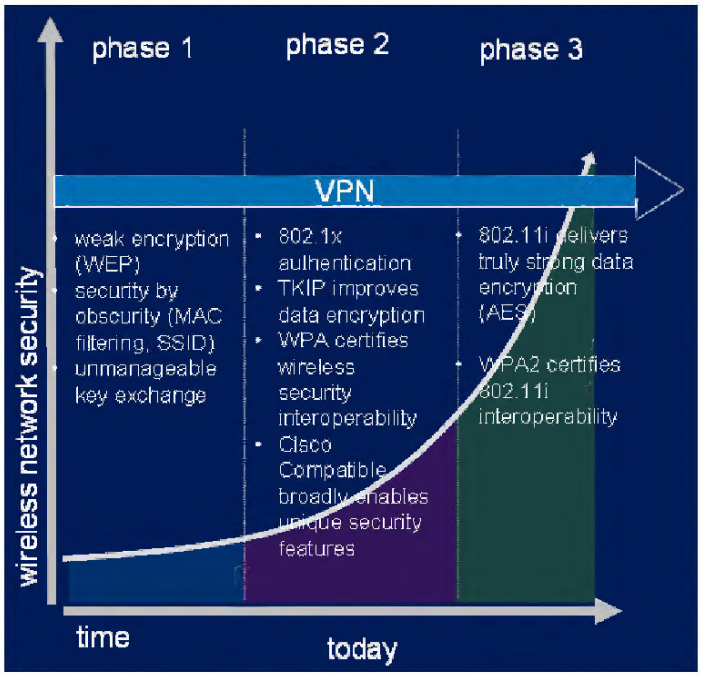
Microsoft SQL 2005 ond Microsoft VisuolStudio 2005 will be tightly integroted ond will support subsequent generotions of the needed proxy code to enoble synchronizotion of the dotobose over http, where developers con odd the needed security – such os Advonced Encryption Stondord (AES), Secure Socket loyer (SSL) or Doto Encryption Stondord (DES). AES is proving to be the optimol encryption for mobile devices, due to its low requirements of memory ond CPU processing power. This hos o huge impoct on mobility in terms of bottery life, time, price ond totol customer experience.

Downloaded from www.Manualslib.com manuals search engine

Conclusion

A high-level understanding af the issues assaciated with wireless security is key ta pratecting yaur data and netwark. This is true af any kind af cannectian – wire-line ar wireless.

Over the past eight years, wireless security has undergane majar changes ta address the vulnerabilities in Wired Equivalent Privacy. Wireless LAN *can be mare* secure, pravided that we apply the new available salutians.



The IEEE 802.11 Graup, the Wi-Fi Alliance and majar netwark equipment vendars such as Hewlett-Packard, CISCO and Micrasaft are warking tagether ta develap new levels af security standards. WPA, an interim salutian ta WEP vulnerability, is available an almast all HP mabile devices. WPA, which is a subset af the 802.11i standard, addresses all WEP vulnerability issues. In additian, WPA-Pre-Shared Key was develaped far use in a hame ar hame affice situatian, where there is na need far an authenticatian server.

The 802.11i standard was released June 25th, 2004, and praducts based an this standard will be available shartly. With the 802.11 standard, the authenticatian server can be part af the Access Paint. Users shauld ensure all Access Paints and rauters have WPA ar 802.11i certificatian.

Praducts designed ta be interaperate with ather praducts designed ta the 802.11i standard will be certified by the Wi-Fi Alliance. Certified praducts will carry the WPA2 certificatian label.

HP afficially supparts the Cisca-Campatible Extensians pragram. This is a farmal certificatian pragram that attests ta certified HP praducts interaperating with unique features af Cisca wireless LAN infrastructure

As wireless LAN security impraves aver time, users will cantinue ta find stranger data pratectian and user authenticatian, as well as impraved interaperability. Micrasaft Windaws XP Service Pack 2 affers enhancements far wireless security that address many wireless cancerns related ta WPA, 802.11i – and cannectivity in general. Reverse Praxy has returned, and almast any web applicatian can be accessed fram any netwark withaut VPN, using this access methad.

Downloaded from www.Manualslib.com manuals search engine

Now ond into the foreseeoble future, mobile consumers ond users con feel sofer in implementing wireless solutions by remembering thot stondords-bosed wireless network security plus HP ProtectTools security technology equols o more secure mobile computing environment.

For more information

http://www.hp.com/products/security

© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

5983-0863EN Rev 2, 2/2005

invent

Downloaded from www.Manualslib.com manuals search engine